Boas Práticas de Segurança: do Commit Até Produção

Cheng Junior

THE DEVELOPER'S CONFERENCE

TEMPEST
Protegendo negócios no mundo digital.

@chengjunior

Vazamento de dados: quase 1 milhão de senhas estão sendo vendidas na internet

O preço exigido pelos criminosos pelas senhas é de "módicos" R$ 9,5 mil

Bancos reforçam segurança contra golpes, que cresceram na quarentena

De novo: vazamento expõe dados de 2 brasileiros

Hackers e exigem

New macOS malware XcodeSpy Targets Xcode Developers with EggShell Backdoor

PHIL STOKES / MARCH 18, 2021

Golpes lic 19 t Wha

Criminosos

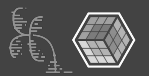
Ataque cibernético mundial levou INSS a suspender atendimento no Brasil

Petrobras, Telefônica, ONS e Tribunal de Justiça de São Paulo também foram atingidos

acker mostra que Brasil ainda não sabe segurança de informação

Causa

- SO (Windows, Linux, MacOS, iOS, Android...)
- Ferramentas
- Engenharia social
- Malware
- Phishing
- Infraestrutura
- Configuração
- Software/Apps



Leis e certificações

LGDP

I - o respeito à privacidade;

II - a autodeterminação informativa;

III - a liberdade de expressão, de informação, de comunicação e de opinião;

IV - a inviolabilidade da intimidade, da honra e da imagem;

V - o desenvolvimento econômico e tecnológico e a inovação;

VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e

VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

ISO 27k

- Normas, guias o boas práticas
- Sistema de Gestão de Segurança da Informação (SGSI)
- ISO 27001 e ISO 27002
  - Segurança de dados digitais
  - Sistemas de armazenamento eletrónico

International Organization for Standardization

BACEN Nº 4.658

BANCO CENTRAL DO BRASIL

- Instituições financeiras
- Empresas autorizadas
- Prestadores de serviços
- Política de segurança
  - Serviços de computação em nuvem
  - Processamento e armazenamento de dados

“devem implementar e manter uma política de segurança cibernética formulada com base em princípios e diretrizes que busquem assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados”

Outras abordagens!!

Atestado [in]segurança

Testes de segurança

(i) Antes de ir pa

- Solicit
- Corrige os
- Retestel?
- Public

(ii) Ataq e em

- Solicita
- Explegue (i)

Abordagem reativa

- Resolve depois
  - Construção
  - Ataque
- Testes tendem ao ∞
- Custo
- Mesmos problemas
- Mesmos riscos

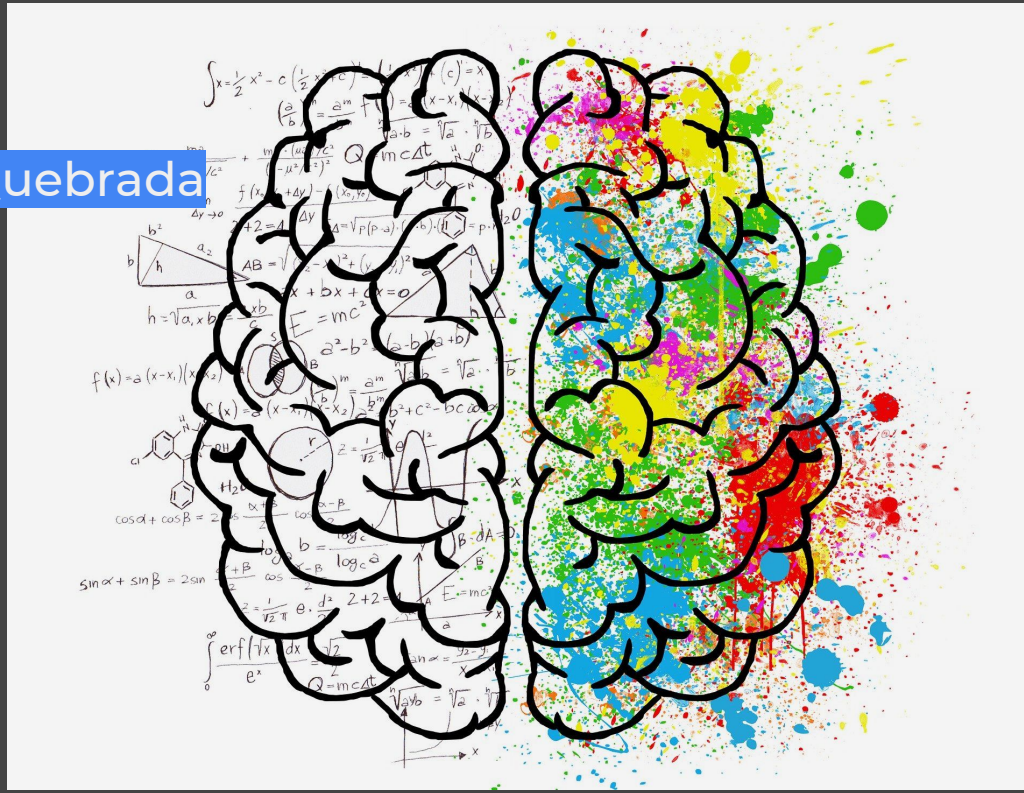
Corrigindo na fonte

Focando na origem

- Arquitetura
- Código
- Processo
- Pessoas

Mindset

- Sempre estará vulnerável
- Não deixe nenhuma Janela Quebrada
- Desconfie e [re]verifique
- Estude Y Estude
- Traga para o dia a dia
- SEMPRE priorize
- Estabeleça seu Nível de Nóia
- Não existe mágica



Hardening

- Trabalho é trabalho...
- Atualize seu SO!!
- Atualize seu navegador!!
- Softwares com procedência
- Informações sensíveis em um cofre
- Configure seu Firewall
- Sua rede não é confiável
- Cubra sua câmera

Stack de desenvolvimento

- Linguagem, Framework, Biblioteca, Banco de dados...
- De acordo com o problema
- Comunidade forte!!
- Histórico de vulnerabilidades e correções
- Assine as listas
- **ATUALIZE!!**
- Não acumule

Treine o time

- Com frequência
- Desenvolvimento Seguro
- Forme ou contrate
- Equalização do conhecimento

Arquitetura e negócio

- Segura por padrão
- Minimamente desacoplável
- Requisitos de segurança
- Destaque o que é crítico

Commit

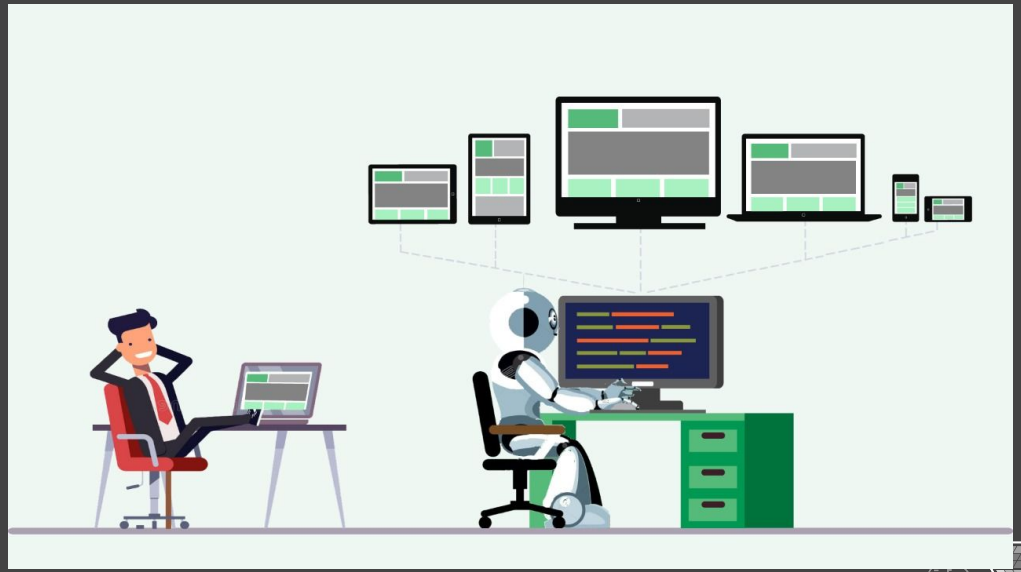
- Com frequência por funcionalidade
- Descrição objetiva
- Trechos de código
- Identificador da tarefa
- **NUNCA** suba informações sensíveis
  - Senha
  - Token
  - No de cartão
  - ...

Revise o código do time

- Por commit (pull request)
- Qualidade e padrão
- Segurança
- Autor != Revisores
- Ferramenta análise estática
- Tempo de revisão (12h? 24h?)

Testes automatizados

- Estabeleça a pirâmide (ex: unitário, integração e API)
- Qualidade != quantidade
- Alta cobertura não é cobrir 100%
- Priorize os cenários críticos
- Pense fora da caixa

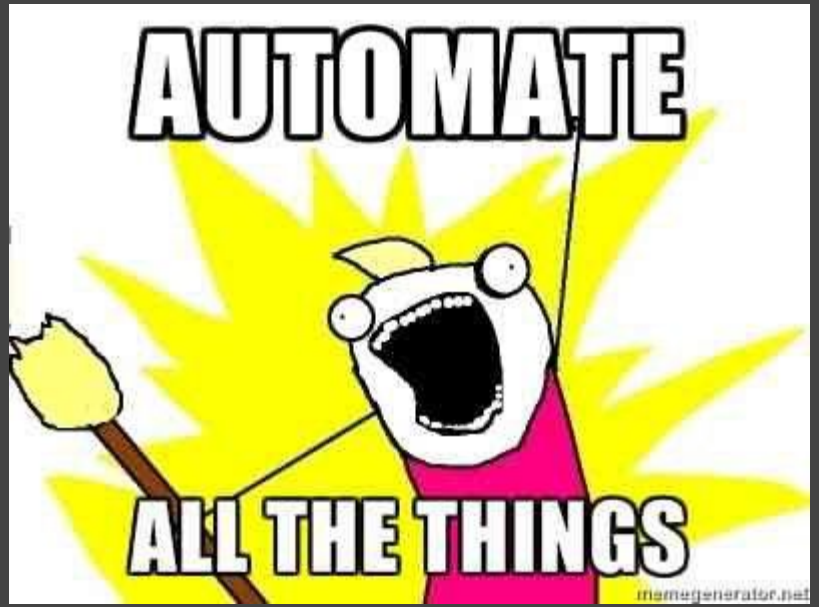


Testes de segurança

- Por sprint, feature, major version...
- Manual por um analista de segurança
- Automatizada por uma ferramenta

Integração contínua

- Pirâmide de testes
- Análise estática do código
- Análise dinâmica p/ ferramenta
- Check de versões
  - Compiladores
  - Frameworks
  - Libs

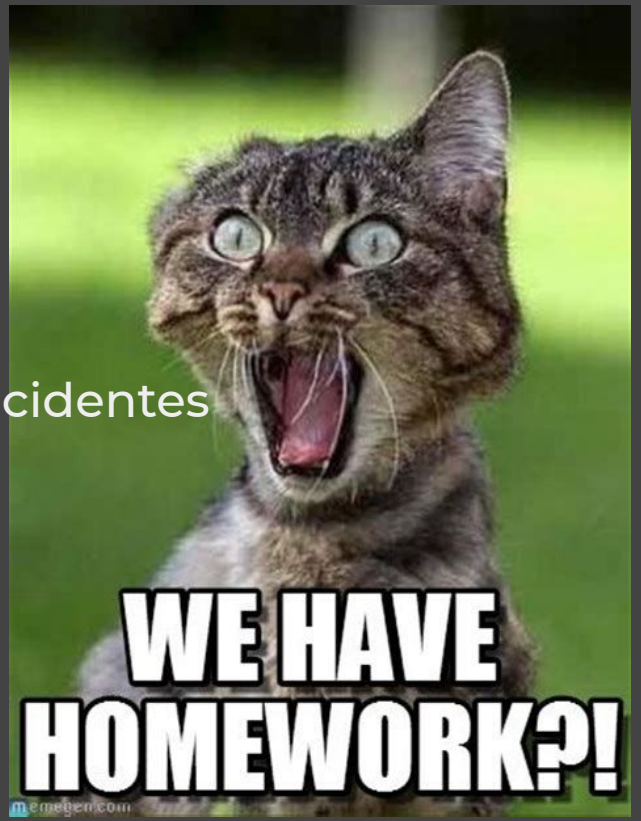


Gerenciamento de acessos

- Privilégio mínimo
- Usuário do banco de dados
- Usuário da app
- Acessos a produção
- Offboarding

Tarefa de casa

- Requisitos de segurança
- Análise de arquitetura
- Modelagem de ameaças
- Desenvolvimento orientado à detecção de incidentes
- Supply chains
- Software Assurance Maturity Model (SAMM)
- OWASP Top Ten
- "The Pragmatic Programmer"
- "Clean Code"
- "The Web Application Hacker's Handbook"



jobs.kenoby.com/tempest/

Temos vagas

Xêro!!

@chengjunior

linkedin.com/in/chengjunior

THE DEVELOPER'S CONFERENCE

TEMPEST

Protegendo negócios no mundo digital.